Ειδήσεις για την ΑΣΦΑΛΕΙΑ στις ΤΠΕ απ' όλο τον κόσμο...

Δελτίο 92
1 Οκτώβρη 2007

NSA to Defend Against Hackers
Baltimore Sun (09/20/07) P. 1A; S. Gorman

The National Security Agency is planning a new "Cyber Initiative," an effort to enlist federal agencies to monitor Internet-based control systems for electricity grids, subways, nuclear power plants, and other infrastructure to prevent unauthorized intrusions. Initially, as many as 2,000 workers from DHS, NSA, and other agencies could be assigned to the project. The plan is a major shift in NSA practices, according to former and current intelligence officials. The new domestic role for the NSA, which traditionally focused on the government's classified networks, would require a revision of the agency's charter. NSA officials would not discuss any specific programs, but did say that cybersecurity is a critical objective for the agency. Cybersecurity has long been an unwanted responsibility, with various federal agencies managing small portions of it, but the NSA, for the most part, was not involved. The Dept. of Homeland Security's first chief of cybersecurity, A. Yoran, says that although the government has made progress, in general federal efforts are "somewhat spotty." One of the biggest problems is that the DHS is responsible for the problem, but does not have the authority or expertise to get other agencies and the private sector to adhere to regulations. Current and former intelligence officials, including several NSA veterans, warn that the new NSA network monitoring program could create new privacy concerns. "If you're going to do cybersecurity, you have to spy on Americans to secure Americans," says a former government official familiar with NSA operations. "It would be a very major step."

Is the US at Risk From Cyberwarfare?
IDG News Service (09/20/07), R. McMillan

Commerce could take a serious hit from cyberattacks, given the degree to which elections, banking, and point-of-sale systems have migrated online. "As we become more networked and more wired, our vulnerabilities increase," notes Center for Intelligence Research and Analysis director J. Mulvenon, who cites the May shutdown of Estonian Internet servers and the subsequent crippling of Estonia's banking system as a case in point. The Homeland Security Department's G. Garcia says preparing for cyberattacks involves many of the same procedures as gearing up for other online threats. "For our purposes, we really need to focus on reducing our vulnerabilities so those attacks don't happen in the first place," he explains. One of the sticking points in plans for the US to wage cyberwarfare against other countries is that such attacks could have a cascading effect that damages civilian systems and services that may not be intended targets. There is also the additional threat of rogue elements who may launch cyberattacks without the approval of their government. Cyberwarfare planners will for now continue to proceed with caution out of concern for unintended consequences, according to Mulvenon.

International Blue Ribbon Task Force to Address Critical Challenge of the Information Age, UCSD News (09/19/07), W. Froelich

A new international Blue Ribbon Task Force on Sustainable Digital Preservation and Access, funded by the National Science Foundation and the A. Mellon Foundation, will work to preserve society's most important digital data. The task force will be assisted by the Library of Congress, the National Archives and Records Administration, the Council of Library and Information Resources, and the Joint Information Systems Committee of the United Kingdom. "It is impossible to imagine success in the Information Age without the availability of our most valuable digital information when we want it now and in the future," says Fran Berman, director of the San Diego Supercomputer Center and UC San Diego and co-chair of the Task Force. "It's critical for our society to have a long-term strategic plan for sustaining digital data and we are excited about the potential for the task force to help form that plan." Berman and co-chair Brain Lavoie, a research scientist and economist with the Online Computer Library Center, will assemble an international group of leaders to develop recommendations for the economic sustainability of digital information. Over the next two years the task force will listen to a broad set of international experts from the academic, public, and private sectors. After two years, the task force will develop a comprehensive analysis of current issues and actionable recommendations to create sustainable strategies for data preservation. "In addition to developing sound technical processes for preserving digital information, we must also ensure that our preservation strategies are economically sustainable," Lavoie says. "The work of the panel will be an important step toward achieving that goal."

Does Antivirus Have a Future?
London Guardian (09/20/07), W. Grossman

The continued effectiveness of antivirus software is in doubt as sneakier, more commercial, and more sophisticated malicious software emerges and is used to launch new kinds of attacks. Antivirus vendors hear such skepticism regularly, and Sophos technology consultant G. Cluley says that regardless of malware's refinement or methodology, its arrival at a computer remains consistent and conventional, in that it is transmitted as a piece of executable code that can be spotted by security software before it can cause harm. Cluley adds that antivirus software's current capabilities may be underestimated by certain parts of the software community, and notes that AV software is in a state of continuous evolution and has become less dependent on virus signatures. Yet a Panda Security poll of 1.5 million consumer PCs found that 37% had fully updated security, and nearly 25% of them were still compromised by malware. AV software is making a transition from blocking bad software to passing only benevolent software, while drive-by attacks--malware that is automatically downloaded when one visits a contaminated Web site--are becoming increasingly common. Malware authors' motivation is also changing, from a desire to hack for the challenge of it or for bragging rights to a desire to turn a profit. University of Auckland researcher P. Gutmann estimates that a talented virus programmer can earn up to $200,000 a year. New viruses are also being designed for stealthiness so that they can linger on a user's system without being spotted, increasing the amount of time they have to wreak havoc. Experts expect security software's deployment and strategy will be rethought, and Columbia University computer science professor S. Stolfo predicts that "eventually, systems implanted in machines will learn your own personal behavior and protect by detecting abnormalities."

Collecting of Details on Travelers Documented
Washington Post (09/22/07) P. A1; E. Nakashima,

The Automated Targeting System has been used to screen travelers since the mid 1990s, but the amount of information gathered and how it is used has changed drastically since 2002,

according to former Dept. of Homeland Security officials. The system is used to collect electronic records on the travel habits of millions of Americans who fly, drive, or take cruises, including information on who they travel with, the personal items they carry, and even the books they bring, according to documents obtained by civil liberty advocates and statements from government officials. The personal travel records are preserved for up to 15 years. A group of civil rights activists requested copies of their own travel records, which included a description of a book on marijuana that one of them carried, and the phone number of one of the activist's sisters in Japan. Dept. of Homeland Security officials, including DHS secretary M. Chertoff, insist that the collection of such information is vital to making connections between possible terrorist suspects, and that the department only gathers information related to possible criminal activities. "I flatly reject the premise that the department is interested in what travelers are reading," says DHS spokesman R. Knocke. "We are completely uninterested in the latest T. Clancy novel that the traveler may be reading." Knocke says that if the traveler's behavior or belongings lead an inspection officer to believe there may be a possible violation of the law, it is the officer's duty to further scrutinize the traveler and to record the incident.

Summit to Address Online Threats to Security
The Tartan (09/24/07), E. Kang

Carnegie Mellon University's CyLab will host the second annual Anti-Phishing Working Group e-crime Researchers' Summit on Oct. 4-5. The summit will feature top e-crime research experts, including Cigital CTO G. McGraw, who will deliver a keynote address on security threats in online multi-player games. "With hundreds of thousands of interacting users," McGraw says, "today's online games are a bellwether of modern software yet to come. The kinds of attack and defense technique I [will] describe are tomorrow's security techniques." The summit will focus on security threats created by massive multiplayer online role-playing games (MMORPG) and phishing, but will also discuss the precautions needed to prevent e-crime and how to determine the risk of a particular threat. McGraw says that MMORPG threaten not only the security of individual players but the welfare of the entire online gaming community. Panelists from the Harvard Center for Research on Computation and Society, Indiana University, and People for the American Way will address the issue of phishing, focusing on how phishing could potentially affect the 2008 elections and how to prevent phishing using both new and old techniques.

Online Game Helps People Recognize Internet Scams
Carnegie Mellon News (09/24/07), B. Spice; A. Watzman

Carnegie Mellon University computer scientists have developed Anti-Phishing Phil, an online fishing game that teaches people how to recognize and avoid email "phishing" attempts and other Internet scams. During testing at the Carnegie Mellon Usable Privacy and Security (CUPS) Laboratory, people who spent 15 minutes playing the game were better able to spot fraudulent Web sites than people who spent 15 minutes reading anti-phishing tutorials and educational material. The lab is now testing the game on the general public through its Web site. Participants are asked to take a short quiz, play the game, and then take another quiz. "We believe education is essential if people are to avoid being ripped off by these phishing attacks and similar online scams," says CUPS Lab director and associate research professor in the School of Computer Science's Institute for Software Research L. Cranor. "Unlike viruses or spyware, phishing attacks don't exploit weaknesses in a computer's hardware or software, but take advantage of the way people use their computers and their often limited know-

ledge of the way computers work." The game managed to improve users' accuracy in spotting dangerous Web sites from 69-87%. "We designed the game to teach people how to use Web addresses, or URLs, to identify phishing Web sites," says PhD student and lead developer of Anti-Phishing Phil S. Sheng.

Apple: 'Unlocking' Software Damages iPhone
USA Today (09/25/07) P. 4B; J. Graham

Apple recently issued a formal statement that said using any software to unlock an iPhone causes "irreparable damage" to the system. Apple also cautioned that such software will cause havoc with the iPhone when it is combined with a new software update that allows iPhone users to access a new feature to buy music downloads through a wireless Internet connection. Previously, Apple has released software updates that prevent others from hacking into its products, but Apple's Phil Schiller says that is not the case with the iPhone. "We tested the phones and discovered that some of these unlocking programs permanently damage software," Schiller says. Some Web sites offer unlocked iPhones for sale, while other sites sell software to allow iPhone owners to unlock the phone themselves. Digital Media analyst P. Leigh says Apple's warning will make consumers think twice before attempting to unlock their phone, but hackers will continue to break the code and find ways around the new software update. "Consumers will scream and yell about this, but in the end, they don't have much of a choice," Schiller says. "The iPhone is a mass-market product, and Apple doesn't want people to circumvent it."

Not Much Anonymity for Unprotected File-Sharers
University of California, Riverside (09/25/07)

University of California, Riverside researchers, in a paper titled "P2P: Is Big Brother Watching You?," show that about 15% of users on file-sharing networks are on the networks to look for illegal file-sharing for the recording industry or the government. "We found that a naive user has no chance of staying anonymous," says UCR graduate student A. Banerjee. "100% of the time, unprotected file-sharing was tracked by people there to look for copyright infringement." However, the research did show that "blocklist" software such as PeerGuardian, Bluetrack, and Trusty Files is fairly effective at creating anonymity, reducing the risk of being observed to about 1%. "Of course no one is suggesting that illegal downloading is a good idea," says UCR computer science professor M. Faloutsos. "But the P2P technology is here to stay and these industries would be better off trying to find ways to provide affordable and convenient alternatives that would allow computer users to download their products legally." UCR's paper was named "best paper" at the International Federation for Information Processing Networking 2007 conference.

Using Spam Blockers to Target HIV, Too
BusinessWeek (10/01/07)No. 4052, P. 68; S. Baker; J. Greene

A team led by Microsoft Research's D. Heckerman set out to build a tool that could block unwanted spam email through the thorough mapping out of thousands of possible spam indicators, and spammers responded to their efforts by modifying these identifiers to get around the blockers, for instance by substituting a "1" for the "i" in "Viagra." This virus-like mutation of spam inspired Heckerman, who is also a physician, to apply the principles behind the spam-blocking technology to the development of software that can detect the AIDS-causing HIV virus. The application of the spam blocker to AIDS research is not so surprising, as many of

Microsoft's researchers stretch into other disciplines regularly. Heckerman analyzes both spam and HIV through the study of statistical relationships in their features, which mutate constantly. The Microsoft scientist draws parallels between spamming methodologies and the infection of cells by HIV, which is done when the virus injects its own genetic material into the cell and then replicates itself by the thousands, spawning mutants that are sometimes drug-resistant. Cells infected by HIV frequently carry mutated "signposts" that cannot be deciphered by immune systems, leading to cases in which drugs that are effective against one form of the virus are ineffective against another form. The hope of Heckerman and his colleagues is that their work could not only be fed into the generation of successful vaccines, but also lead to an effective tool for damming the deluge of junk email.

US Video Shows Simulated Hacker Attack
Associated Press (09/27/07), T. Bridis; E. Sullivan

A video made by the Idaho National Laboratory for the Homeland Security Department depicts an electrical turbine catching fire to illustrate what could happen if hackers launched an attack on the US electrical grid. The videotaped simulation, known as the "Aurora Generator Test," was produced by researchers probing a hazardous vulnerability in US utility companies' computers; the programming flaw has since been repaired. According to experts, the electrical equipment that runs the country's water, power, and chemical plants is "very old technology." Moreover, security issues were not taken into consideration when such systems were originally designed. Years ago, top telecommunications advisers to President Bush asserted that an organization could electronically carry out an attack on the electric power grid from a remote location and with a great deal of anonymity. The Idaho National Laboratory confirmed such a possibility, dubbing it "the invisible threat." However, other industry experts note that criminals would require specialized information--such as how to deactivate warning systems--to conduct such an attack. Regardless, the Homeland Security Department and electrical companies have been collaborating to improve security measures, and to date "we've taken a lot of risk off the table," says R. Jamison of the Homeland Security Department. In addition, the Federal Energy Regulatory Commission put forward a series of standards in July 2007 that, if implemented, would safeguard the nation's electric power supply system from cyberattacks by mandating the creation of plans and controls.

MIT Launches Kerberos Consortium
MIT News (09/27/07), P. Richards

MIT on Thursday announced the launch of the Kerberos Consortium, a joint effort on the part of industry and academia to create a universal authentication program based on Kerberos to protect computer networks. "By establishing the Kerberos Consortium, MIT seeks to permit Kerberos to continue to grow and develop as a stable and universal 'single sign-on' mechanism for the users of modern computer networks," says Kerberos Consortium executive director S. Buckley. Kerberos Consortium chief technologist S. Hartman says the objective is to make Kerberos more useful and available. "We foresee a day when Kerberos-based authentication and authorization will be as ubiquitous as TCP/IP-based networking itself," Hartman says. One of the consortium's primary objectives is to provide the solutions it promotes as open source reference implementations that can be used by consortium members in their products and organizations without licensing fees. "We see a number of our customers asking for open source, stable, and interoperable single-sign on technology, based on the Kerberos protocol," says Sun Microsystems director K. Jenks. "The MIT Kerberos Consortium is an

outstanding way to address our customers' requirements, and a continuation of the work we have been doing within the Kerberos community over the last several years."

Online Biometrics Flaw Gives Hackers a 'Fake Finger'
New Scientist (09/24/07), A. Ananthaswamy

Researchers in Germany have discovered that the "fuzzy vault" cryptographic scheme requires too much computing power and can be broken in a day using a desktop computer. The biometrics strategy was seen as a way for people to use their fingerprints to log into online bank, email, and other accounts. A more advanced level of cryptography, the "fuzzy vault" made the transmission of an encrypted fingerprint possible because the print scanned by a user's PC would not have to look exactly like the match stored by a Web site. The system is designed to store a user's fingerprint on a secure database as a list of coordinates for specific features, create a list of number pairs comprised of the real coordinates and their encrypted partners, and generate thousands of fake versions to disguise them. Researchers had believed that a hacker would not be able to pick out the real coordinates among the numerous fake pairs. However, an analysis by P. Mihailescu at the University of Gottingen that involved about 500 fake versions suggests otherwise. A hacker could use the coordinates to create a fake finger and impersonate someone "for a lifetime," says Mihailescu.